PATENT APPLICATION
Docket No.: 5045.2.1D

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Vincent S. Darago and Christopher Jenkins
Serial No.:	10/609,325
Filed:	June 27, 2003
For:	Computer architecture for managing courseware in a shared use operating environment

RESPONSE

Honorable Commissioner for Patents:

Applicant respectfully submits the following Response to the Office Action mailed March 9, 2007.

Double Patenting

A Terminal Disclaimer signed by the undersigned attorney of record is enclosed.

Section 103 and Claim 86

With regard to the Section 103 rejection of claim 86, the undersigned appreciates the opportunity to explain how the present invention differs from the cited references. Diligent examination strengthens patents.

Among other things, claim 86 requires "disabling caching and other disk writes to prevent a copy of the critical portion of the content from being created on nonvolatile storage at the client workstation". The Office Action acknowledges that Wiser does not teach this feature. Instead, the rejections rely on the assertion that Schell (US 6477648) teaches this feature at column 2 lines 43-44 and 56-59. The Office Action argues that it would have been obvious for one skilled in the art to combine this teaching of Schell with the asserted teachings of Wiser "in order to disable write to prevent license information being sent and received or copied at the client's computer". The undersigned respectfully disagrees with the rejection.

First, it is unlikely that one of skill would have combined Schell with Wiser, given the evident tension between their purposes. Wiser seeks widespread delivery of music to consumers (Abstract), whereas Schell provides restricted communications to protect confidential information in businesses such as banking, brokerage, and government entities (col. 1 lines 36-60).

But even if Wiser and Schell had been combined, they would not teach the present invention. Schell does not teach "disabling caching and other disk writes to prevent a copy of the critical portion of the content from being created on nonvolatile storage at the client workstation". Column 2 of Schell states, beginning at line 7:

> The NIC comprises a send address confirmation circuit which contains a trusted source address (e.g., a medium access control (MAC) address or a network layer address) uniquely associated with the trusted workstation. In general, the source address can be any address that identifies the source of a packet, including for example the MAC address, Internet address, transport layer address or session layer address, etcetera. For each packet transmitted from the trusted workstation over the network, the NIC checks the source address inserted in the packet by an NIC driver to ensure that this driver-inserted source address matches the trusted source address. Thus, if untrusted software on the workstation attempts to transmit a packet with a source address other than the trusted source address, the NIC prevents the packet from being transmitted. This prevents malicious attempts by a hacker/attacker to forge packets from a workstation with another workstation's source address.
>
> The NIC also includes a receive address confirmation circuit that functions to ensure that the trusted workstation does not receive packets from entities other than known/authorized servers. That is, the NIC compares the source address of a packet received over the network to verify that it is from a authorized server. Significantly, if each workstation on a network is populated with a NIC, the known/authorized servers will control all packets on the network and can trust the source of all requests.
>
> The send and receive address confirmation circuits are trusted because the contents of registers resident in these circuits are written to and modifiable only during a pre-boot state, which is the only time the untrusted elements (e.g., untrusted software on the workstation) are not accessed. That is, following a hardware reset and prior to execution of the operating or application software on the workstation, enforcement registers with the send and receive conformation circuits are written to with source address data, and then write disabled to prevent subsequent loading of unauthorized source address data.

> Specifically, following a hardware reset of the workstation, the NIC is initialized and pre-boot modules are downloaded to the workstation over the network from a known server under the control of instructions resident in an adapter BIOS on the NIC. The NIC may be located on an expansion board separate (e.g., ISA or PCI compatible) from the workstation motherboard, or on the motherboard. Once the pre-boot modules are down loaded to the workstation, the pre-boot modules are executed to perform a login--identification and authentication (I & A) function for the user and to load the enforcement registers with the send and receive trusted source address information. The enforcement registers are then locked (i.e., write disable) to prevent the contents of the send and receive enforcement registers from being modified until another hardware reset occurs. Once execution of the pre-boot modules is complete, the NIC BIOS transfers code execution to a workstation system BIOS to complete the initialization of the workstation.

That is, Schell teaches that a register holding a source address in a network interface card (NIC) is write-disabled after being written to a single time with a source address following a hardware reset and prior to execution of the operating or application software on a workstation, so that the trusted workstation does not receive packets from entities other than known/authorized servers. Even if Schell's technology were used in an embodiment of the present invention, it would not disable caching and other disk writes of information already present on the workstation. Stopping data from being received at a workstation, as in Schell, is not at all the same as stopping data already received at the workstation from being permanently stored on a disk, as called for in claim 86.

There are also other problems with trying to apply Schell's teachings to the present invention. Schell contemplates a hardware reset, then one write to a register – before the operating system or applications run, and then no further writes to that register. At least some embodiments of the present invention, by contrast, contemplate a finished boot process (whether caused by a hardware reset or simple powering up), with the loading of an operating system and application software, which then downloads critical portions and other data, and which allows some writes to disk while disallowing others, to prevent unauthorized nonvolatile copies of critical portions but allow such copies of other data. Thus, the timing, the nature, and the scope of Schell's write disablement all pose problems

for use in the present invention. They are clearly very different than what is called for in claim 86.

For at least these reasons, the rejection of claim 86 should be withdrawn.

Section 103 and Claims 87-106

With regard to the Section 103 rejection of claims 87-106, which rely on combining Salesky (US 6343313) with Wiser, independent claim 87 requires "peer-to-peer nodes" and also requires "serving at least the critical portion over a network communications link to a peer node". But neither Salesky nor Wiser even mention "peer" nodes. For at least this reason, the rejections should be withdrawn.

Conclusion

Assignee respectfully requests allowance of the claims. Some objections to the Office Action assertions that could be made have not been, since the reasons given above are sufficient to require withdrawal of the rejections. In the event of any questions, the undersigned invites a telephone call from the Office.

Dated May 14, 2007.

Respectfully submitted,

\pm1-5045-2-1D

CERTIFICATE OF TRANSMISSION

I hereby certify that this Response, Terminal Disclaimer, and fee are being submitted to the Commissioner for Patents through EFS-WEB, on May 14, 2007.

JOHN W. OGILVIE
Registration No. 37,987
Attorney for Assignee

OGILVIE LAW FIRM
1320 East Laird Avenue
Salt Lake City, Utah 84105
801-706-2546 (voice)
801-583-0393 (fax)